REMARKS

Claims 1-15 were pending and were rejected. Claims 1, 3, 9, 13, 14, 15 have been amended. New claims 16-18 have been added. Claims 4, 5, 7 and 8 have been canceled.

In the Office Action, the examiner rejected the claims based on 35 USC 101 and the examiner also rejected the claims as unpatentable based on a lack of nonobviousness under 35 USC 103(a) citing US 7272625 to Hannel in view of US 6321267 to Donaldson.

General Differences Between Claimed Invention and Hannel

In contrast to Hannel and the prior art, the claimed invention allows for precise list customization of each user account. For every user the claimed invention has a separate list. All the access lists separately configure for each and every user. The fact that the claimed invention utilizes exception lists corresponding to each user account list also provides significant advantages since it allows for prudent use of wild characters. The use of wild characters for defining a set is wildly popular in computer science, but it normally tends to slows down computing speed.

Use of range and wild characters determine a set of resources, where all elements within the range (including delimiters) and all possible elements within the wild character are in the resource set. Two examples of the use of wild characters are provided below:

1) Set of 234.*.43.67 has a possible 256 IP addresses (elements) within the following delimiters as:

Starting From IP is: 234.0.43.67

Ending To IP: 234.255.43.67

2) Set of 2* from all two digit numbers has a possible 10 elements within the following delimiters as:

Starting From: 20

Ending To: 29

Regarding the use of wild character in resource identifications, Hannel does not allow the corrective measure of an exception list. For example, Hannel addresses such a use of "IP Range," where the starting IP and the ending IPs determine a range of affected IPs for resources. See, e.g. Hannel Figure 13A. The use of exception lists in the claimed invention, in contrast, makes the use of "resource range" or wild characters more flexible, and customizable, and allows you to accurately personalize the account for large sets of resources.

Another nonobvious difference of the claimed invention is its deterministic customization – that the same result is obtained even if you change the order of the rules being applied. In general, policy management systems are hard to configure in a deterministic way. Notwithstanding the difficulty, the claimed invention is deterministic. Policy management, list processing and user account customization is based on strictly friendly or unfriendly setups, only one of which is active at any given time and hence results in deterministic customization and access management.

In Hannel, in contrast to the prior art, the policy management system performs nondeterministic actions. That is because both approved and

disapprove actions are possible within the system. See, e.g. Figure 11 of Hannel, where group "gr1" is given "Deny", and group "gr2" is given "Allow" actions.

Another novel difference (see claims 3 and 17) is that for domain filtering there can be a privacy shield for outbound communications

Another novel difference is that in the claimed invention for domain filtering there can be partial name of domains and partial IP addresses for friendly and unfriendly lists. For example, defining "XXX" to be an unfriendly list item, then all the following resources will be denied access as:

www.abcXXXefg.com*

www.XXXbcaad.us*

ndXXX.tv*

Similar example can be presented for partial IP addresses (such as "56.34") for unfriendly user access list item, then all the following resources will be denied access as:

http:\\129.56.34.**

http:\\56.34.*.37*

http:\\198.*.56.34*

However, Hannel resource database does not present such partial matching capabilities, and it is not intuitive to use such design. See Hannel Figs. 13A, 14, It can be seen that Hannel uses a domain which is different from partial domain name of the claimed invention. Hannel also uses IP filtering and IP, but he does not speak of partial IP address as resources, as the claimed

invention does.

Specific Response

The examiner stated in the Office Action summary that the examiner rejects claims 1-14. The examiner stated in a telephone conversation with Applicant's counsel that this was a typo and he intended to also reject claim 15. Item 5 of the Office Action section "Detailed Action" states that the examiner rejects claims 1-3 and 6-14 but then goes to refer to claims 1 and "13-15". In any event, the Office Action rejects claim 9 which recites the encryption limitation that appears in claim 15.

Amended independent claim 15 and amended dependent claim 9 teach the novel and nonobvious feature of a symmetric encryption function being capable of encrypting only a portion of an email text as well as the idea of a text editor for editing purposes. This is not taught by the prior art including by Hannel.

In rejecting claim 9, which contains the encryption function of claim 15, the examiner cited Hannel, column 35, lines 20-22 and column 34, lines 1-24. These portions of Hannel merely establish a type of encryption. Unlike the claimed software, however, Hannel does not teach the idea of an encryption function being capable of encrypting only a portion of an email text or only a portion of an email attachment. The significance of this capability is discussed explicitly in, and hence is supported by, the third Object and Advantage on page 5 of the Specification as well as the Detailed Description of the Specification at pages 16 line 19 through page 17 line 15 from which the quote below is taken.

"Software 10 has a special encryption utility that can evade data mining programs... The encryption component or function is capable of encrypting at the user's option all or only a portion of an e-mail message and all or only a portion of an e-mail message attachment file. ... The binary key is very good for encrypting files on a hard drive, which protects against intrusion attack. By encrypting only a minimal portion of an e-mail message or its attachment file or a combination of files, the data mining engines are evaded since such engines have recognition tools that recognize the main or most prevalent text that appears in a file or message. Accordingly, when the data mining engine sees that most of the text of the e-mail message, the e-mail attachment file or the combination of files are not encrypted, the data mining engine does not signal that the message or file(s) is something it does not understand since it may be encrypted. On the other hand, since it in fact does not understand the small portion that was encrypted, it ignores that small portion."

Accordingly, the use of partial encryption has major advantages for protecting confidentialities and will evade the eavesdroppers who are looking for valuable information within email channels. Such eavesdroppers will be alarmed by seeing fully encrypted. That raises a flag for them. However partial encrypted emails do not raise suspicious activity alerts.

Furthermore, the type of encryption in Hannel is public/private encryption rather than symmetric encryption.

Moreover, Hannel's "Adaptive encryption" is not the partial text encryption as taught by the claimed invention, and certainly not partial text encryption at the option of the user who selects text within the email message. Rather, in Hannel, the client resource requesting messages and the responses are encrypted when necessary and in accordance with Hannel "VPN" standards, and in accordance with the "trust level" balanced against data sensitivity. If, for example, the message security requirement level is low, Hannel's design will bypass encryption of messages up to the IP filters. Thus, the rules are set depend on the data sensitivity factor defines by the type of resources and administrators.

The encryption is not set by decisions of a user at his option.

Claims 1 and 13 have been amended to add the limitation that was previously recited in canceled claim 7 (with the exception that "appoved users" was changed to "clients of approved users" and "unapproved users" was changed to "clients of unapproved users", see below). It is respectfully submitted that this limitation is not taught by the prior art notwithstanding the examiner's assertion in discussing claim 7 that Hannel teaches this limitation at column 39 lines 1-25. Furthermore, one of the novel and nonobvious aspects of this limitation resides in the fact that "clients of approved users are listed in the application server in the unfriendly inbound list and are sent by the application server to the replacement location, and wherein clients of unapproved users are not listed in the unfriendly inbound list and have their request sent to a published address that contains harmless information". This is counter-intuitive. One would certainly expect clients of approved users to be listed in the friendly list and clients of unapproved users to be listed in the unfriendly list. Neither Hannel nor any other prior art reference teaches or suggests this in the context of the other limitations.

Hannel in the column and lines cited by the examiner merely refers to access management rules and adjusting the trust levels. It certainly does not describe the unique claimed manner of configuring approved and unapproved users with unfriendly and friendly lists. Furthermore, access filter 203 of Hannel supports actions which are not customizable per user account whereas in the claimed invention all lists are uniquely configured for each account, i.e.

everything is user customizable.

With respect to claims 13 and 14, soft content filtering also contains novel and nonobvious aspects. As described in the Summary of the Invention in the Specification of the claimed invention, soft content filtering is defined to result in highlighting (see page 4 of Specification 3rd to last line stating: "if the soft filtering approves the content then it highlights the content"). Moreover, the user chooses this feature. The fact that when soft content filtering is executed against corresponding friendly content lists, the list items will be highlighted within the accessed document has very significant advantages, since it can be used for intelligent searches, where a user may only get access to relevant documents with highlighted strings indicating the relevance of particular paragraphs. The highlighted documents have great user interactive effects. See Specification at page 13, last paragraph – to page 14, first paragraph. Hannel, does not provide soft filtering within the same context. Neither does Donaldson teach or suggest this, including at column 41, lines 46-55 the portion that was cited by the examiner.

Applicant has also amended claims 1 and 13 to move from approved users to clients of approved users and from unapproved users to clients of unapproved users. This is supported by the parent patent application (incorporated by reference in the instant application) on page 10 (first full paragraph) where it states that approved users are listed by the host (client) name.

The examiner has issued an Office Action dated December 16, 2008

responding to the September 29, 2008 Amendment stating that this amendment fails to explain how new claims 16-18 are distinguishable over the prior art. In response to the December 16, 2008 Office Action Applicant states that new claim 16 is dependent on independent claim 15 as to which Applicant argued is distinguishable over the prior art (see above at page 20 of the instant Amendment and see above at pages 17-20 of the instant Amendment for general discussion). Since claim 15 is distinguishable over the prior art, claim 16, which is dependent on claim 15, is also distinguishable over the prior art.

Furthermore, claim 16 teaches the novel idea of being able to encrypt only a portion of an e-mail message attachment file. Rather than encrypting a large attachment file in its entirety or a large email, only a few sensitive words need be encrypted. As shown in the Specification at page 2 line 6, page 5 item (3) and pages 16 line 20 through page 17 line 15, this provides significant advantages for at least two reasons. First, such partial encryption on sensitive documents and emails messages where only a few words of an email or attachment are sensitive allows protecting minimal information just enough to support confidentiality with minimal computer power usage. Second, such minimal encryption capability will better confuse data mining engines that may parse all documents and emails sent and received at the corporate boundaries for data collection on a brute force fashion. Such minimal encrypted texts will hide critical information without raising red flags at the interception engines for further audit purpose. This is because the overall text body will be parsed successfully to human readable languages (using dictionaries), and thus the text will not be found suspicious – with the

exception of a few encrypted strings which may be regarded by those parsing engines as possible mistaken words and thus none conforming to any meaningful word. While such data mining engines will only collect information that is not harmful, they will not raise red flags for further audits on the user communications. If the entire email text or attached text were encrypted, the data mining engines will find them unreadable by any available dictionary, and thus, they would send alerts for further user audits.

Regarding new claim 18, this claim is dependent on claim 13 and Applicant argued extensively is distinguishable over the prior art (see above at pages 22-23 of the instant Amendment and see above at pages 17-20 for general discussion). Since claim 13 is distinguishable over the prior art, claim 18, which is dependent on claim 13, is also distinguishable over the prior art. Furthermore, claim 18 teaches the novel idea of "the content filtering engine, when performing hard filtering, [being able to] replace a requested document that has been rejected with a replacement document selected by a user of the administrator account." It is respectfully submitted that this is not taught in the cited prior art in the context of the present invention and may have at least the following advantages.

First, this allows fine account customization for portal purposes, where such configurations are managed at the intermediate nodes such as corporate gateways rather than the service provider portals. This allows corporate to adapt external and internal resources suitable for their employees on the top of the service provider's portal configurations per individual users. Second, the power

to customize resources allows user secure access to their service provider portals by allowing per user look-and-feel customization to authenticate the portal site to the user. This prevents fishing attacks. For example, as part of multi-factor authentication, many financial sites provide pre-selected images and letters passed to the users. Empowering intermediate nodes such as proxies to perform such content alterations allows more efficient anti-phishing techniques as well as proxy authentication to the user. Third, there are other occasions where page alteration at the proxy allows corporate, as well as parents to change the resource with less harmful resources, or remove/alter available links and objects on the accessed original resources. Fourth, the use of proxy/intermediate nodes for such resource alterations (requested web resources) is also suitable for demographics customization of service sites with heavily traffics, where the site's resources may not be customized efficiently on real time requests, and due to demographics attributes. Fifth, language and localization support will be more efficiently implement at the intermediate traffic nodes such as proxies. For example, a proxy server intercepting a popular site such as www.cnn.com who is requesting the page in East Africa may see advertisements set for that part of the continent and language than www.cnn.com page available to users from East Asia (China,) and other users from East Asia (Vietnam). The proxies for such regions will efficiently change the CNN sites and pages suitable for those users.

Finally, regarding new claim 17, this claim is dependent on claim 14. Furthermore, claim 14 teaches the novel idea that the content filtering engine has

an inbound privacy shield for blocking scripting language functions for particular user accounts. The list customization per user account supports fine-grain user account customization. Each user account has its own setups. Hard and soft content filtering produces different filtering results. This fine level of customization is not taught anywhere in the prior art in the context of the present invention.

Applicant has also amended page 5 of the Description to clarify that the Objects and Advantages may be present in certain embodiments.

It is respectfully requested that the above amendments be entered and that claims 1-3, 6, 9-18, which are understood to be in condition for allowance, be allowed.

Previously, a credit card authorization form for payment of $65 for a response within the first month was submitted and in addition, previously, a credit card authorization form for $600 previously accompanied the September 29, 2008 Amendment to cover payment of $75 for one new dependent claim as well as $525 for payment in connection with a response within the third month.

Dated: June 11, 2009

Respectfully submitted,

Steven Horowitz, Attorney for Applicant
Registration No. 31,768
295 Madison Avenue, Suite 700
New York, NY 10017
(212) 867-6800
(212) 685-6862 fax
sh@patentny.com